

Amendments to the Specification:

Please amend the paragraph on page 4 of the application, at lines 4-13, as follows:

The foregoing and other objects of the invention are achieved by providing a system and method wherein a media provider acquires digital information of interest to at least one user of a host system. The digital information may be any type including one or more image, audiovisual/movie, and/or text files. These files may be personally related to the user or be of more general appeal. In order to encourage the user to buy the information, the media provider takes steps to ensure that the user has only temporary or partial access to the information when reproduced on the host system. This access control is performed based on a plurality of types of decryption keys sent from the provider to the user, and a media player application which is able to recognize each type of decryption key sent from the provider.

Please amend the paragraph bridging pages 16 and 17 of the application, beginning on page 16 at line 15, as follows:

Alternatively, the key(s) could be placed in a completely separate file. This file could have, for example, a name and location of the customer's choosing, so that the customer would know where to find it. As a further alternative, the key(s) may be embedded in the application, just as other program data. A further approach involves storing critical data in a place designated for such use by the operating system. For example, the Windows operating system has an entity called the "registry," which is used by the operating system but any application may add to, delete from, or read registry information (commonly referred to as "keys" or "values"). Keys might not be stored on the host system at all, but instead may be always dynamically fetched from a network. In this latter situation, the playback function of the media player is subordinate to the network being functional and

responsive.

Please amend the paragraph on page 19 of the application, at lines 5-11, as follows:

In all the foregoing embodiments, the threshold conditions for controlling reproduction quality degradation (e.g., time conditions, numbers of playbacks, etc.) are set by the media provider, and comparisons are made with respect to this information before playback. (Block 316). Those skilled in the art can appreciate that the specific conditions discussed above, while beneficial, are merely illustrative and that other conditions may be set for controlling reproduction quality in accordance with the present invention.

Please amend the Abstract on page 43 of the application, at lines 5-18, as follows:

A method for controlling access to digital information is performed based on a plurality of decryption keys sent by the information provider. A first type of decryption key instructs a user's host system to reproduce the digital information in accordance with a first level of reproduction quality degradation. Additional keys may specify other degradation levels. The quality of the digital information may be degraded based on a time condition or a use condition. Alternatively, only a portion of the information may be made viewable by a user. In order to obtain full and unrestricted access, the user must obtain a type of decryption key from the provider which removes all previous limitations on reproduction quality degradation. Preferably, the digital information is sent with a media player application program embedded with an initial decryption key. The program may include tamper-resistant features which provide a safeguard against hackers or other forms of unauthorized access. A business method uses a pricing structure which makes the decryption keys available for different prices.